

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

CHIEF JUDGE EDMUND A. SARGUS, JR.

IN THE MATTER OF THE SEARCH OF:

Contents and records relating to the Google
Accounts (Google Plus, Gmail, Google Drive)
Related to the e-mail addresses:

which are stored at premises controlled by
Google, Inc., 1600 Amphitheatre Parkway,
Mountain View, AC 94043

OPINION AND ORDER

This matter is before the Court on the Government's Motion for Reconsideration of what the Government has deemed a denial of an application for a search warrant.¹ For the reasons set forth below, the Court **DENIES** the Government's Motion for Reconsideration. Based on the extraordinary circumstances of this case, the Court withdraws the order of reference for this warrant under 28 U.S.C. § 636, Federal Rule of Criminal Procedure 59(a), and Local Rule 72.2. This Court finds that the records sought are within the scope of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.* The application for a search warrant is **GRANTED**.

I.

On February 12, 2018, an Assistant United States Attorney and a Homeland Security Investigations Task Force Officer presented an application for a search warrant to a Magistrate Judge in the United States District Court for the Southern District of Ohio, Eastern Division. The search warrant application sought electronic communications and records related to a

¹ As described herein, this Court disagrees with the Government's characterization that the application was denied.

defendant's Google email accounts, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) of the SCA. The warrant sought to require Google to disclose all responsive information, regardless of whether it is "stored, held or maintained inside or outside of the United States."

Upon review of the search warrant and accompanying documents, the Magistrate Judge found probable cause to issue the warrant. This Court, reviewing the warrant request and supporting affidavit, also finds probable cause exists. Before signing, the Magistrate Judge inquired as to why an Addendum, which had heretofore been submitted with other similar applications, was not attached. The Addendum required Google to preserve, but not provide, "responsive information stored solely outside of the United States."²

The Government objects to the Addendum, deeming the request a denial of its application for a search warrant, and asks the Court to find the decision clearly erroneous or contrary to law. *See* 28 U.S.C. § 636(b)(1)(A) ("A judge of the court may reconsider any pretrial matter under this subparagraph (A) where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law.").

This Court has serious doubt as to whether there is an order of the Magistrate Judge capable of review by the undersigned. No written order has been issued; no briefing has been considered by the Magistrate Judge.

Even assuming the existence of a reviewable order, this Court cannot find that the Magistrate Judge's action was clearly erroneous or contrary to law. As described *infra*, the only federal appellate court to address whether the SCA authorized a warrant to obtain electronic records in another country has found that the statute does not extend beyond the United States.

² The proposed Addendum, attached to the Government's motion, would have required Google to notify the United States Attorney of the location of information stored outside of the country. Google could then move to quash or the Government could move to compel. In either case, the matter would have been briefed and formally ruled upon.

See In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporations, 829 F.3d 197 (2d Cir. 2016) (“*Microsoft I*”), *reh’g denied*, 855 F.3d 53 (2d Cir. 2017) (“*Microsoft II*”). As will be discussed, other courts have disagreed and the matter is currently before the United States Supreme Court. *United States v. Microsoft Corp.*, 138 S. Ct. 356 (2017) (“*Microsoft III*”). The referenced Addendum would have the practical effect of preserving the information sought and, most likely, would set up a focused briefing of the issue. This did not occur and the Magistrate Judge made no final ruling on the scope of the SCA. There is no clearly erroneous decision that is contrary to law.

II.

Given the unique circumstances of these issues, which are certainly capable of repetition, and the fact that major service providers subject to orders under the SCA have fully explored all legal arguments in filings before the Supreme Court and in *Microsoft I, II*, all of which this Court has reviewed, the undersigned finds there is substantial jurisprudential value in deciding the matter and providing a modicum of certainty, prior to a final decision of the Supreme Court. Applications for warrants under the SCA are made with great frequency, as email communications replace regular mail. In many cases, simply waiting for a decision from a pending Supreme Court case is prudent. The issue in this case implicates numerous other investigations, many of which are no doubt time sensitive.

The SCA was enacted as Title II of the Electronic Communications Privacy Act of 1986 (“ECPA”). The ECPA regulates government access to wire and electronic communications. 18 U.S.C. § 2510 *et seq.* Under the SCA, the Government may compel a service provider to disclose the contents of electronic communications, including emails, or other records and information within its control. 18 U.S.C. § 2703. In interpreting the SCA, the Second Circuit in

Microsoft I reversed the district court's denial of Microsoft Corporation's motion to quash a warrant issued under the SCA, which directed Microsoft to produce the contents of an email account that it maintained for a customer. A United States Magistrate Judge had issued a warrant on the Government's application, having found probable cause to believe that the account was being used in furtherance of narcotics trafficking. The warrant was then served on Microsoft at its headquarters in Redmond, Washington. Microsoft ascertained that, to comply fully with the warrant, it would need to access customer content that it stored in Ireland. The Court of Appeals for the Second Circuit held in *Microsoft I* that the Government was not entitled to the seizure of responsive records or communications because the information was stored abroad.

The United States petitioned the Second Circuit for a rehearing *en banc* in *Microsoft II*. The entire Second Circuit split evenly on the request, which left the panel decision intact. *Microsoft II*, 855 F.3d at 60 (Jacobs, J., dissenting). Precisely half of the members of Second Circuit disagree with the panel decision in *Microsoft I*. On October 16, 2017, the Supreme Court granted a *writ of certiorari* in the case and the matter is scheduled for oral argument later this month.

No other circuit, including the Sixth Circuit, has addressed this issue. The Second Circuit's decision in *Microsoft I* has been rejected by the numerous other courts considering the issue, including a sister district court from this circuit. *See, e.g., United States v. Google, Inc.*, Case No. 17-mc-7 (W.D. Tenn. Nov. 3, 2017) (sealed) (determining relevant conduct within Section 2703's focus, occurs in the United States); *In re Info. Associated with @gmail.com*, Case No. 16-mj-757, 2017 U.S. Dist. LEXIS 130153, 2017 WL 3445634, at *27 (D.D.C. July 31, 2017) ("the SCA warrant [is] simply a domestic execution of the court's statutorily authorized

enforcement jurisdiction over a service provider, which may be compelled to retrieve electronic information targeted by the warrant, regardless of where the information is ‘located;’”), *aff’g* 2017 WL 2480752 (D.D.C. June 2, 2017); *In re Search Warrant No. 16-960-M-1*, Case No. 16-cr-960, 2017 U.S. Dist. LEXIS 131230 (E.D. Pa. Aug. 17, 2017) *aff’g* 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017); *Matter of Search of Content Stored at Premises Controlled by Google Inc.*, Case No. 16-mc-80263, 2017 WL 3478809, at *5 (N.D. Cal. Aug. 14, 2017), *aff’g* 2017 WL 1487625 (N.D. Cal. April 25, 2017) (“the information sought by the government is easily and lawfully accessed in the United States, and disclosure of that content would likewise take place in the United States”); *In re Search of Information Associated with Accounts Identified as [Redacted]@gmail.com*, Case No. 16-mj-2197, 2017 WL 3263351, at *9 (C.D. Cal. July 13, 2017); *In re Information associated with one Yahoo email address that is stored at premises controlled by Yahoo/In re: Two email accounts stored at Google, Inc.*, Case No. 17-M-1234 and 17-M-1235, 2017 WL 706307, at *3 (E.D. Wis. Feb. 21, 2017) (determining that what matters in the execution of a SCA warrant compelling disclosure by a service provider is the location of the service provider).

The Second Circuit held in *Microsoft I* that the SCA lacks extraterritorial reach, and that there is a presumption against applying a federal law beyond the territorial boundaries of the United States. *See Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010) (federal laws construed to have only domestic application, agent clearly expressed congressional intent to the contrary). One of the dissenters in *Microsoft II* wrote that “no extraterritorial reach is needed to require delivery in the United States of the information sought, which is easily accessible in the United States at a computer terminal.” *Microsoft II*, 855 F.3d at 61 (Jacobs, J., dissenting). As Judge Jacobs noted:

Extraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant. The warrant in this case can reach what it seeks because the warrant was served on Microsoft, and Microsoft has access to the information sought. It need only touch some keys in Redmond, Washington. If I can access my emails from my phone, then in an important sense my emails are in my pocket, notwithstanding where my provider keeps its servers.

Id. The same holds true with the Government’s request to Google in the instant action.

In contrast, the *Microsoft I* court engaged in an analysis of extraterritoriality and determined that the SCA’s focus lies on protecting user privacy. This “determination was made under the second part of the extraterritoriality analysis set forth as a canon of construction in *Morrison* and recently developed further in *RJR Nabisco, Inc. v. European Community*, — U.S. —, 136 S.Ct. 2090 (2016). *See RJR Nabisco*, 136 S.Ct. at 2101 (“If the statute is not extraterritorial, then at the second step we determine whether the case involves a domestic application of the statute, and we do this by looking to the statute’s ‘focus.’”).” *Microsoft II*, 855 F.3d at 55–56. Thus, “[t]he second step of the two-step framework for analyzing extraterritoriality issues set forth in *Morrison v. National Australia Bank Ltd.* . . . and *RJR Nabisco, Inc. v. European Community* . . . was the determinative issue in [*Microsoft I*].” *Microsoft II*, 855 F.3d at 65 (Cabrane, J., dissenting).

The decision then shifted to the focus of the SCA. “At step two, a court must ‘determine whether the case involves a domestic application of the statute,’ which ‘we do . . . by looking to the statute’s ‘focus’ and by identifying where “the conduct relevant to the statute’s focus occurred.” *Id.* at 65–66. *Microsoft I* concluded that the “‘focus’ of the SCA is user privacy, and . . . the location of the conduct relevant to that focus . . . ‘takes place under the SCA where the customer’s protected content is accessed—here, where it is seized by Microsoft,’” which was in Ireland. *Id.* at 66. In *Microsoft II*, Judge Cabranes offered a persuasive retort:

Even if the “focus” of the SCA is user privacy, a plain reading of the statute makes clear that the conduct relevant to the SCA’s “focus,” and which the SCA seeks to regulate, is a provider’s *disclosure* or *non-disclosure* of emails to third parties, not a provider’s *access* to a customer’s data. Here, Microsoft’s disclosure of emails to the government would take place at its headquarters in the United States. Therefore, had the panel majority correctly identified the conduct relevant to the SCA’s “privacy focus,” it would have concluded that the warrant at issue was a domestic application of the SCA.

....

Put another way, Microsoft did not need a warrant to take possession of the emails stored in Ireland. Nor did it need a warrant to move the emails from Ireland to the United States. It already had possession of, and lawful *access* to, the targeted emails from its office in Redmond, Washington. Only Microsoft’s *disclosure* of the emails to the government would have been unlawful under the SCA absent a warrant.

Id. at 66–68.

Judge Droney, also dissenting from the denial of a rehearing *en banc* in *Microsoft II*, noted that the *Microsoft I* privacy concerns were unpersuasive because “Congress addressed those concerns through the warrant requirement in the SCA.” *Id.* at 75 (citing 18 U.S.C. § 2703). He explained:

That requirement provides protection for individual privacy interests by requiring the Government to make an adequate showing of probable cause of evidence of a crime or property used to commit a crime to a judge—a well-established standard of Fourth Amendment protection. *See id.*; Fed. R. Crim. P. 41(c); U.S. Const. amend. IV (“[N]o warrants shall issue, but upon probable cause.”); *Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967) (explaining that purpose of Fourth Amendment’s probable cause requirement “is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials”).

....

It makes no difference that Microsoft has chosen to store some electronic communications in other countries. That decision is based on its own business considerations, not privacy concerns for its customers. Microsoft has possession and immediate access to those emails regardless of where it chose to store them. Thus, the second prong of the *RJR Nabisco* test is satisfied here: the disclosure of

the electronic communications occurs in the United States, when Microsoft honors the warrant by disclosing those communications.

Id. at 75–76 (parallel citations omitted).

The final consideration relates to the effects of the decision in *Microsoft I*. Judge Cabranes noted in dissent in *Microsoft II* that “regardless of whether they are controlled by a domestic service provider and are accessible from within the United States . . . the government can ‘never obtain a warrant’ that would require a service provider to turn over emails stored in servers located outside the United States, regardless of how ‘certain [the government] may be that [emails] contain evidence of criminal activity, and even if that criminal activity is a terrorist plot.’” *Id.* at 63–64.

Second, *Microsoft I* “has created a roadmap for even an unsophisticated person to use email to facilitate criminal activity while avoiding detection by law enforcement,” because if a customer indicates he or she resides abroad, emails are then stored abroad. *Id.* at 64.

Third, and last, *Microsoft I*

. . . has already led major service providers to reduce significantly their cooperation with law enforcement. The panel majority held that the physical location of a server containing a customer’s emails determines whether an SCA warrant seeking the disclosure of those emails is an extraterritorial application of the SCA. However, electronic data storage is more complex and haphazard than the panel majority’s holding assumes. Many service providers regularly “store different pieces of information for a single customer account in various datacenters at the same time, and routinely move data around based on their own internal business practices.” Still other providers are unable to determine “where particular data is stored or whether it is stored outside the United States.” Consequently, in an effort to apply the panel majority’s confected holding to the technological realities of electronic data storage, major service providers are adopting.

Id. Judge Cabranes offers two examples of the “baleful consequences” of following *Microsoft I*:

Google will now disclose “only those portions of customer accounts stored in the United States at the moment the warrant is served.” Google’s policy is particularly troubling because “the only [Google] employees who can access the entirety of a customer’s account, including those portions momentarily stored

overseas, are located in the United States.” As a result, law enforcement might never be able obtain data stored in Google servers abroad, even with the help of [a Mutual Legal Assistance Treaty].

Yahoo! has advised law enforcement that it “will not even preserve data located outside the United States in response to a [s]ection 2703 request.” This policy, as the government points out in its *En Banc* Petition, creates “a risk that data will be moved or deleted before the United States can seek assistance from a foreign jurisdiction, much less actually serve a warrant and secure the data.”

Id. at 64–65.

Thus, reading the SCA to prohibit the disclosure of foreign-stored data would undermine an important tool for law enforcement and introduce arbitrariness to the statutory scheme.

Google’s network automatically moves some of its users’ data—including emails that contain attachments, and the attachments themselves—around the world, at various times, depending on the workings of a computer algorithm aimed at creating network efficiency. *See In re Search of Information Associated with [Redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 2480752, at *3; *In re Search Warrant No. 16-960-M-01 to Google*, Case Nos. 16-960-M-1 and 16-1091, 2017 WL 471564, at *3–4 (E.D. Pa. Feb. 3, 2017). The operation of Google’s network shines a light on *Microsoft P*’s flawed rationale, which focuses on the geographic location of data instead of the act of production in the United States. Google’s compliance with a § 2703 warrant requiring it to produce information stored in the United States—but not information stored abroad—would depend on the happenstance of where the data is located at the precise moment when the warrant is served or the provider accesses its network. *See In re Premises Controlled by Google, Inc.*, 2017 WL 2480752 at *2. Because Google’s data does not persist in any one geographic location, a restrictive reading of § 2703 would impede countless criminal investigations.

This Court notes its agreement with Judge Droney, who commented that *Microsoft I* “undertook the daunting task of attempting to apply a statute enacted decades ago to present technology.” *Id.* at 74. (Droney J., dissenting).

For example, who knew in 1986 that electronic mail—“email”—would become such a primary means of communication that its commercial providers would have millions of servers across the world to store and manage those communications? Or that the recipient of the warrant here—Microsoft—would itself manage over one million server computers, located in over forty countries, used by over one billion customers? Such developments in electronic communications could not have been anticipated at the time of the statute’s adoption. Indeed, the task of applying statutes and rules from many years ago to unanticipated advances in technology has been undertaken in other contexts with much difficulty. *See, e.g., United States v. Ganius*, 824 F.3d 199, 219–21 (2d Cir. 2016) (*en banc*).

Id. at 74–75.

A thirty-year old statute still governs the authority of the federal courts to order production of the electronic records in criminal investigations. While much of the law involves reasoning by analogy, the pace and extent of technological changes makes such tasks much harder. The Court concludes this opinion with one final stab at applying traditional legal principles to an internet driven era.

Before and after the advent of the internet, no federal court could order a seizure or production of property or paper beyond the territorial limits of the United States. Yet, if a bank in Columbus, Ohio held copies of records, the originals of which were in Ireland, no one would seriously contend that the copies in Columbus were beyond the reach of a federal warrant. Emails of an American citizen stored by an American corporation located within the territorial jurisdiction of the United States are no different. What is sought can be obtained within the United States by an American corporation. No federal agent will ever set foot in another country in order to comply with the warrant herein sought.

III.

Based on the foregoing, the Court **DENIES** the Government's Motion for Reconsideration. Due to the nature of the issues raised herein, the Court it withdraws the order of reference under 28 U.S.C. § 636, Federal Rule of Criminal Procedure 59(a), and Local Rule 72.2 for this particular warrant and determines that the warrant shall be issued for the Government to obtain the email communications from Google.

IT IS SO ORDERED.

2-15-2018
DATE


EDMUND A. SARGUS, JR.
CHIEF UNITED STATES DISTRICT JUDGE